NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

North Dakota

Minot changes flood model. The Grand Forks Herald reported February 4 that U.S. officials, including the North Dakota governor, were talking with Canadian officials about changing the operational plan for the dams that both sides agreed to in 1989 to account for torrential rain. They also proposed raising Lake Darling Dam, the one dam that is on the U.S. side, and building a system of dikes and diversions in the Minot, North Dakota area similar to the one built in Grand Forks after the 1997 flood. The 2011 flood, which forced the evacuation of 11,000 in Minot alone, has changed the historic model. The week of January 30, North Dakota officials said they met with the Saskatchewan premier to talk about amending the 1989 agreement so rainfall would be accounted for, and the premier agreed In North Dakota, the governor is seeking more flexibility by pushing for an upgrade to Lake Darling Dam to store more water. He said in a January statement after a meeting in Minot that bot U.S. Fish and Wildlife, which owns the dam, and the U.S. Army Corps of Engineers, which controls it during flood operations, are open to the idea. Source: http://www.grandforksherald.com/event/article/id/228569/group/homepage/

Regional

(Minnesota) **Xcel's Prairie Island nuclear plant in Minnesota vents tritium.** Xcel Energy Inc.'s Prairie Island nuclear plant in Red Wing, Minnesota, released 27 gallons of radioactive water in a leak from its condenser system, according to a filing with the Nuclear Regulatory Commission (NRC) February 7. The 27 gallons of condensate was released from a steam system overflow vent and return pumps failed to operate, causing an overflow onto the ground at the plant, February 3. Despite the incident, the plant's two reactors were operating at full power. The release contained 15,000 picocuries per liter of tritium, a low-level radioactive form of hydrogen. The Environmental Protection Agency's drinking water standard allows 20,000 picocuries per liter, according to the NRC. The leak also included methoxypropylamine, ammonia, and hydrazine, the filing showed. Source: http://www.bloomberg.com/news/2012-02-07/xcel-s-prairie-island-nuclear-plant-in-minnesota-vents-tritium.html

(Montana) **Feds: Few pipeline plans account for river risks.** Federal officials investigating a pipeline break that spilled 1,500 barrels of oil into a Montana river said February 8 few companies take river erosion and other risks into account when evaluating pipeline safety. In recent months, several companies have completed or made plans for significant upgrades to pipelines across major waterways in Montana and adjoining parts of Wyoming and Idaho. Among those were an estimated $20 million in improvements to Exxon's 12-inch Silvertip line, which broke July 1 during flooding on the Yellowstone River, fouling about 70 miles of shoreline. But more must be done, said the western region director for the federal Pipeline and Hazardous Materials Safety Administration. Montana has 6,700 miles of natural gas transmission, oil, and other hazardous liquid pipelines and another 6,683 miles of smaller distribution lines that connect to service lines for homes and businesses. The state averages about six or seven serious accidents on those lines annually. There are 82 points at which oil and other hazardous liquid pipelines cross major rivers in Montana and portions of adjoining states. Inspections in the wake of the Yellowstone spill found exposed sections of pipe or other problems at eight of those major crossings and many smaller river and stream crossings. Source: http://missoulian.com/news/state-and-regional/feds-few-pipeline-plans-account-for-river-risks/article_d70bb73e-5297-11e1-ace2-0019bb2963f4.html

National

Nothing Significant to Report

International

Dam bursts in Bulgaria, 8 killed in floods. A dam in southern Bulgaria burst February 3 after days of heavy rain, bringing the toll from the region's flooding to eight dead, 10 missing. The dam on the Ivanovo Reservoir collapsed, sending an 8-foot torrent into 700 houses in the village of Bisser near the Greek border, the civil defense chief said. Four bodies were found in the raging waters, the mayor reported. Authorities have declared a state of emergency in much of southern Bulgaria. The district governor said four were killed and 10 people are still missing in floods that have washed away bridges and roads. The government warned Turkey and Greece of massive floods surging down the Arda, Tundzha, and Maritsa rivers. The civil defense agency also warned that two dams at Ivaylovgrad and Studena were on the brink of overflowing and urged residents to prepare for an evacuation. Landslides derailed the engine of an Istanbul-bound train near Svilengrad, causing no injuries but leaving at least a dozen foreigners stuck for hours, officials said. Source: http://www.boston.com/news/world/europe/articles/2012/02/06/dam_bursts_in_bulgaria_floods_village_and_kills_3/

Watermelon Salmonella outbreak in UK, Europe. An outbreak of Salmonella Newport in six countries that has sickened 54 and killed one has been tentatively linked to ready-to-eat sliced watermelon imported from Brazil, Food Safety News reported February 4. The outbreak began in December, 2011. The UK's Health Protection Agency is still investigating the outbreak, and officials said they cannot yet conclusively link the outbreak to sliced watermelon. Between 10 and 15 victims reported eating the fruit within 2 or 3 days of falling ill. The breakdown of the cases by country: England (26), Germany (15), Republic of Ireland (5), Scotland (5), Wales (3), and N. Ireland (1). Source: http://www.foodsafetynews.com/2012/02/watermelon-salmonella-outbreak-in-uk-europe/

Banking and Finance Industry

States, banks reach foreclosure-abuse settlement. U.S. states reached a landmark $25 billion deal February 9 with the nation's biggest mortgage lenders over foreclosure abuses. The deal requires five of the largest banks to reduce loans for about 1 million households at risk of foreclosure. The lenders will also send checks of $2,000 to about 750,000 Americans who were improperly foreclosed upon. The banks will have 3 years to fulfill the terms of the deal. Federal and state officials announced at a news conference that 49 states had joined the settlement.

Oklahoma announced a separate deal with the five banks. Under the deal, the states said they will not pursue civil charges, however homeowners can still sue lenders in civil court, and federal and state authorities can pursue criminal charges. Critics note the settlement will apply only to privately held mortgages issued from 2008 through 2011. Mortgage held by Fannie Mae and Freddie Mac are not covered by the deal. Lenders that violate the deal could face $1 million penalties per violation and up to $5 million for repeat violators. Bank of America will pay the most as part of the deal — nearly $8.6 billion. Wells Fargo will pay about $4.3 billion, JPMorgan Chase roughly $4.2 billion, Citigroup about $1.8 billion, and Ally Financial $200 million. Those totals do not include $5.5 billion that the banks will reimburse federal and state governments for money spent on improper foreclosures. The deal also ends a separate investigation into Bank of America and Countrywide for inflating appraisals of loans from 2003 through most of 2009. Under the deal, banks are barred from foreclosing on a homeowner who is being considered for a loan modification. The banks and U.S. state attorneys general agreed to the deal late February 8 after 16 months of contentious negotiations. Source: http://www.google.com/hostednews/ap/article/ALeqM5jya_VBd_x6jiXTTNU5HB_IZsa3XQ?docId=8b513ae763564e2a8440252ffbee2874

Anonymous says it knocked Citigroup sites offline. Hackers claiming to be members of the loose hacking collective Anonymous took credit for knocking the Citigroup and Citibank Web sites offline February 3. At times the sites were only sporadically available, and some attempts to log into banking accounts were met with an error message. A Citigroup spokesman confirmed Citigroup's consumer site had experienced a temporary outage, but said the bank was able to restore Web site operations within ` hour and was continuing to monitor its systems. This was part of a recent string of attacks by hackers who call themselves Anonymous Brazil. In posts on Twitter, the hackers said their attacks were intended to fight corruption. By February 3, they had at various times taken down the Web sites of Banco BMG, Banco Bradesco, Banco de Brasil, Banco Panamericano, Citigroup, HSBC Holdings, Itau Unibanco Banco Multiplo, and Febraban, Brazil's banking federation. Source: http://bits.blogs.nytimes.com/2012/02/03/anonymous-says-it-knocked-citigroup-sites-offline/

Hackers may be able to 'outwit' online banking security devices. An investigation by BBC Click underlines possible shortcomings in the extra security provided by banking authentication devices such as PINSentry from Barclays and SecureKey from HSBC. Hackers could set up a fake banking Web site and prompt users attempting to log into their account for both their online log-in credential and, for example, a PINSentry code. This information would allow cybercrooks to log onto the genuine banking Web site, posing as a customer, before authorizing fraudulent transfers or other payments. This variant of a classic man-in-the-middle-attack is know in security circles as a man-in-the-browser attack. Isolated incidents of this type of fraud have cropped up over recent years. While the attack is not new, it is doubtful that many consumers are aware of it. Source: http://www.theregister.co.uk/2012/02/06/online_banking_security/

Chemical and Hazardous Materials Sector

(Georgia) **NRC approves first new nuclear plant since '78.** The nation's first new nuclear power plant in a generation won approval February 9 as federal regulators voted to grant a license for two new reactors in Georgia. The Nuclear Regulatory Commission (NRC) voted 4-1 to approve Atlanta-based Southern Co.'s request to build two nuclear reactors at its Vogtle site south of Augusta. The vote clears the way for officials to issue an operating license for the reactors, which could begin operating as soon as 2016 and 2017. The NRC last approved construction of a nuclear plant in 1978. Source: http://www.wytv.com/news/national/story/NRC-approves-first-new-nuclear-plant-since-78/r0LRmBFcoEmdtsoCnUYj0g.cspx

Study says nuclear plant designs need stepped-up attention to security. A report by a group of nuclear scientists said there is room to enhance new reactor and plant designs. The extensive report "The Future of Nuclear Power in the United States," released February 8 by the Federation of American Scientists and Washington and Lee University, said while most safety procedures and precautions at U.S. nuclear plants are geared towards accidents, more attention must be paid to intentional attacks and sabotage. The study's senior researcher noted the terror threat to nuclear plants comes primarily in two types: ground-based armed attacks, and asymmetric attacks using brute force or cyber vulnerabilities. He also said spent fuel pools are generally not protected by a containment dome and are more vulnerable than the reactor to attacks from the ground or air. Ways to manage the spent fuel pools — such as more rapid removal of spent fuel to dry-cask storage, or, by carefully interspersing hotter and cooler spent fuel could reduce the vulnerability. Source: http://www.gsnmagazine.com/node/25600?c=infrastructure_protection

CFATS can be fixed, DHS officials tell skeptical House Republicans. DHS officials emphasized progress in a troubled program overseeing chemical facility safety before a skeptical audience of Republican lawmakers during a February 3 hearing. "Bad news is something we can do something about," said the head of the DHS National Protection and Programs Directorate, while before the House Energy and Commerce Subcommittee on Environment and the Economy. He oversees at a high level the Chemical Facility Anti-Terrorism Standards (CFATS) program; an internal review conducted in late 2011 found it suffered from a lack of trained personnel, inadequate spending controls, and other problems. Another investigation in summer 2011 found CFATS program officials in May 2010 had improperly classified the risk levels of some facilities due to faulty computer modeling made with improper inputs. New risk level assessments resulted in 148 facilities being downgraded to a lower level, and 99 facilities being excluded from CFATS regulation altogether. DHS officials said CFATS had improved its performance over the past few months. From November 28 through January 28, the program office conditionally authorized site security plans at 43 Tier 1 facilities, one official said, whereas in the previous 23 months, it had conditionally authorized only 10. In prepared testimony, the head of oversight of CFATS said the program has likely resulted in more than 1,600 facilities completely removing chemicals of interest, and more than 700 other facilities reducing their holdings. Source: http://www.fiercehomelandsecurity.com/story/cfats-can-be-fixed-dhs-officials-tell-skeptical-republicans/2012-02-06

Commercial Facilities

Nothing Significant to Report

Communications Sector

(California) **4 Wildomar men caught stealing microwave tower.** Four men were allegedly caught stealing a microwave tower from a Wildomar, California property February 6, causing several thousand dollars in damage. The men were arrested around 5:45 a.m. after allegedly dismantling the transmission tower, according to the Riverside County Sheriff's Department. Deputies were called to the location to investigate a report of trespassing and caught the suspects in the act, a police sergeant alleged. He said the owner of the microwave transmitter, American Tower, estimated the damage to be in excess of $3,000. All of the men were booked on suspicion of commercial theft and vandalism. Source: http://www.swrnn.com/2012/02/06/4-wildomar-men-caught-stealing-microwave-tower/

Firms could see PCs lose internet access in DNSChanger switch off. Firms were warned that some of their users could shortly lose the ability to connect to the Internet or access e-mails, as law enforcers turn off a DNS-rerouting system. The system was established to help victims of the Rove Digital cybercrime syndicate, which distributed malware capable of changing victims' DNS settings to point to rogue servers run by the group. The FBI managed to close down the DNSChanger criminal operation, and secured funding to run the malicious servers until March 8, using the servers to point those with infected machines to their intended destination. The DNSChanger Working Group (DCWG) is currently deliberating whether to seek an extension to its funding. A decision to withdraw the service could see 450,000 users — many of them in large multinational enterprises — losing their ability to connect to the Internet. Source: http://www.v3.co.uk/v3-uk/news/2144194/firms-pcs-lose-internet-access-dnschanger-switch

Critical Manufacturing

NHTSA recall notice - Nissan Versa automatic transmission components. Nissan announced February 10 the recall of 36,608 model year 2012 Versa vehicles equipped with an automatic transmission and manufactured from June 9 through January 13 for failing to comply with federal motor vehicle safety standards related to theft protection. Due to interference between the shifter rod and the shift knob, the vehicles may be shifted out of the park position without depressing the brake pedal. The operator can inadvertently shift the vehicle into gear without the brake pedal being depressed, increasing the risk of a crash or injury to a nearby pedestrian. Nissan will notify owners, and dealers will inspect and replace the shifter knob or the shifter assembly as needed. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V032000&summary=true&prod_id=1312775&PrintVersion=YES

NHTSA recall notice - Volvo VHD, VNL, and VNM trucks brake relay valves. Volvo announced February 9 the recall of 22,383 model year 2011-2012 VHD and model year 2011-2013 VNL and

VNM heavy trucks manufactured from December 2, 2010 through January 18, 2012, and equipped with Bendix ATR-6 traction relay valves. In extremely cold conditions, these Bendix relay valves may potentially develop internal leakage. Internal leakage can lead to air pressure being delivered to affected primary or secondary brakes causing continuous brake application. Inadvertent brake application can cause the brakes to overheat and lead to a fire. It can also cause the wheels to lock up, leading the driver to lose control of the vehicle, increasing the risk of a crash. Volvo will notify owners, and provide a temporary repair until Bendix develops a permanent remedy. Source: http://www-odi.nhtsa.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V036000&summary=true&prod_id=982768&PrintVersion=YES

NHTSA recall notice - Ford F-53 and F-59 automatic transmission selector cable. Ford announced February 8 the recall of 13,239 model year 2011 F-53 and F-59 stripped chassis vehicles manufactured from February 1, 2010 through July 1, 2011, and from May 10, 2011 through October 25, 2011. The 'PRNDL' cable may break at the attachment to the transmission control selector arm assembly mounted on the steering column. If the cable breaks, the transmission gear indicator in the 'PRNDL' display in the instrument panel will remain in the first gear position regardless of the gear selected. An incorrect gear indication in the instrument panel may prevent the driver from knowing if they are in park or reverse, increasing the risk of a crash. Ford will notify owners, and dealers will replace the transmission selector arm assembly and the 'PRNDL' cable assembly. Source: http://www-odi.nhtsa.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V035000&summary=true&prod_id=1421768&PrintVersion=YES

Fire concerns prompt York International to reannounce recall of gas furnaces for manufactured homes. The U.S. Consumer Product Safety Commission and Health Canada, in cooperation with York International Corp., February 3 announced a voluntary recall of 223,600 (in the United States) Coleman, Coleman Evcon, and Red T gas furnaces for manufactured homes, as well as 2,400 additional units in Canada. The units were originally recalled during 2004, but may still remain in use. The furnace can overheat and cause the heat-exchanger to crack and create openings that allow flames to be exposed. When this happens, drywall and other nearby combustibles are exposed to the flames, posing a fire and smoke hazard to consumers. York International has received reports of 393 incidents, including some involving extensive property damage that could be related to these hazards, 366 of those reports were received after the initial November 2004 recall announcement. The units were sold nationwide between 1995 and 2000. Consumers should immediately stop using the furnace until it has been inspected and repaired. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12102.html

NHTSA recall notice - Kenworth and Peterbilt trucks brake relay valves. Paccar is recalling 15,932 model year 2012 and 2013 Kenworth T and W series, and Peterbilt 300 and 500 series heavy trucks manufactured from January 31, 2011 through January 19, 2012 and equipped with Bendix ATR-6 antilock traction relay valves. In extremely cold conditions, these valves may potentially develop internal leakage. Leakage can lead to air pressure being delivered to affected primary or secondary brakes, causing continuous brake application. Unexpected continuous brake application can cause the brakes to overheat and lead to a fire. It can also cause the driver to lose control of the vehicle, increasing the risk of a crash. Also, the brakes may be applied without illuminating the brake lights, failing to give proper warning to other drivers. Paccar will notify owners, and provide a temporary repair until Bendix develops a permanent remedy. The safety recall is expected to begin during February 2012. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V026000&summary=true&prod_id=1116771&PrintVersion=YES

Boeing to correct 787 Dreamliner fuselage issue. Boeing announced in a statement February 5 they have discovered a problem related to the aft fuselage of its 787 Dreamliner planes and are making repairs that will not affect production of the aircraft. “Boeing has found that incorrect shimming was performed on support structure on the aft fuselage of some 787s,” a Boeing spokesman said. He added, “we do not expect that it will affect our planned product rate increases,” and that there are no short-term safety concerns. He declined to comment on how many aircraft were affected. Source: http://www.chicagotribune.com/business/breaking/chi-boeing-investigates-fuselage-problem-on-new-dreamliner-787s-20120206,0,958507.story

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

(Alabama; Texas) **Hackers breach Alabama and Texas law enforcement sites.** As part of their operations against law enforcement agencies, Anonymous hackers breached the sites of the Alabama Department of Public Safety, the Texas Department of Public Safety, and the Mobile Police Department, also based in Alabama, leaking information from their databases, Softpedia reported February 10. DataBreaches summed up the hacks, revealing the hackers managed to obtain tons of sensitive data, but published only enough to prove the sites are vulnerable, making sure no innocent individual suffers. The main hackers were CabinCr3w and w0rmer, but it seems they were assisted by Kahuna in the breach that targeted the Mobile Police Department. The database contained information on offenders such as ID, case number, names, physical descriptions, and other data, but the hackers redacted all the sensitive information. From the public safety departments of Texas and Alabama there was not much data leaked, except for a few database structures, the hackers urging the site’s administrators to patch them up. DataBreaches notified the Mobile Police Department of the hack. Source: http://news.softpedia.com/news/Hackers-Breach-Alabama-and-Texas-Law-Enforcement-Sites-251967.shtml

(Alabama) **Patrol cars targeted in break-ins; weapons taken.** Law enforcement officials believe an organized group is responsible for stealing weapons, bulletproof vests, and ammunition from several patrol cars in several counties in Alabama, the Gadsden Times reported February

6. At least 11 weapons, including AR-15 assault rifles, were taken from law enforcement vehicles since December 2011, the sheriff said. Seven patrol vehicles were broken into, including five the weekend of February 4. The weapons were stored in the patrol cars' trunks, and the cars' windows were broken out to gain access to open the trunk. The vehicles broken into over the weekend were from one side of the county to the other, prompting law enforcement officials to believe the group split up and hit some of the vehicles about the same time. The sheriff said the FBI, the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives, and the U.S. Marshals Gulf Coast Regional Fugitive Task Force are assisting in the investigation. Source: http://www.gadsdentimes.com/article/20120206/NEWS/120209898/1017/NEWS?p=1&tc=pg

Great Central U.S. ShakeOut earthquake drill drawing more participants in Oklahoma this year. More than four times as many Oklahomans have registered to participate in the Great Central U.S. ShakeOut earthquake drill as did last year. The drill was scheduled for 10:15 a.m. February 7, at which time individuals would simultaneously practice recommended earthquake safety actions. So far, about 47,000 Oklahomans have registered for the ShakeOut, in comparison to fewer than 10,000 in April, said a spokeswoman for the state emergency management department. The ShakeOut will take place in communities throughout the Central U.S. Earthquake Consortium member states of Alabama, Arkansas, Illinois, Indiana, Kentucky, Mississippi, Missouri, and Tennessee. These are the states most at risk from damaging earthquakes along the New Madrid Seismic Zone. Source: http://newsok.com/great-central-u.s.-shakeout-earthquake-drill-drawing-more-participants-in-oklahoma-this-year/article/3646013?custom_click=pod_headline_europe

(Massachusetts) **Boston Police Dept. Web site still offline.** Boston, Massachusetts police hope to have their Web site's blog up and running later February 6 as they continue investigating into the hacking of their Web site. Last week, the group known as Anonymous claimed credit for posting videos and songs showing police brutality on the department's site. The group said they did it in retaliation for the way the Boston Police Department treated Occupiers. Most of the site has been restored. Source: http://www.myfoxboston.com/dpp/news/local/boston-police-dept-web-site-still-offline-20120206

Energy

Utilities facing brute-force attack threat. The Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT) reported February 3 that many organizations have been witnessing secure shell (SSH) scans of their Internet-facing control systems, including an electric utility that told ICS-CERT it was hit by some brute force attempts against its networks that were "unsuccessful." The attackers are probing Port 22/TCP, the default SSL listening port, to look for SSH. Once the attackers get a response from the probe, they can execute a brute-force attack for log-in credentials to acquire remote access. SSH is an attractive attack vector because many control-system devices on networks run it by default. ICS-CERT recommends monitoring network logs for port scans and access attempts. Source:

http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232600345/

Food and Agriculture

Big spinach recall with no public notice. On December 31, a Texas company recalled 228,360 lbs. — 114 tons — of spinach because it tested positive for E. coli O157:H7, Food Safety News reported February 10. That Class I recall — which the U.S. Food and Drug Administration (FDA) defines as “a situation in which there is a reasonable probability that the use of or exposure to a violative product will cause serious adverse health consequences or death” — was revealed as an item in the FDA enforcement report February 8. The potentially contaminated spinach from Tiro Tres Farms of Eagle Pass, Texas, was distributed in Colorado, Kentucky, Massachusetts, and Pennsylvania, and in Canada in Ontario and Quebec. FDA and the Canadian Food Inspection Agency did not publish public notices of this recall in December or January — and still have not — and the FDA enforcement report did not say whether there were any illnesses linked to the recalled spinach. According to the enforcement report, Tiro Tres Farms notified its own customers of the recall by letter December 31, but the FDA report does not indicate if any of the spinach was sold by retailers. The recall was of Robert’s S 1 cut leaf “Curly” spinach. Source: http://www.foodsafetynews.com/2012/02/major-spinach-recall-with-no-public-notice/

FSIS delays ‘Big Six’ E. coli policy 90 days. The U.S. Department of Agriculture’s new non-O157 E. coli policy, which classifies six new strains as adulterants and requires testing, will become effective 90 days later than originally planned, the Food Safety and Inspection Service (FSIS) announced February 8. The delay will push back the routine sampling of the six additional STEC serogroups, O26, O45, O103, O111, O121, and O145, to June 4, from the original deadline of March 5. The agency is planning to initially sample raw beef manufacturing trimmings and other raw ground beef product components produced domestically and imported, and test the samples for the serogroups. If these products test positive for non-O157 STECs, they will be prevented from entering commerce — in the same way that E. coli O157: H7 has been treated since 1994. According to the Centers for Disease Control and Prevention, the six additional strains of E. coli being targeted cause about 113,000 illnesses and 300 hospitalizations annually in the United States. Source: http://www.foodsafetynews.com/2012/02/new-e-coli/

Fast-spreading animal virus leaps Europe, UK borders. A newly identified disease is moving rapidly through livestock in Europe and has authorities worried and puzzled, Wired reported February 7. The disease, dubbed Schmallenberg virus for a town in west-central Germany where one of the first outbreaks occurred, makes adult animals only mildly ill, but causes lambs, kids, and calves to be born dead or deformed. The United Kingdom’s Animal Health and Veterinary Laboratories Agency (AVHLA) said February 7 the virus has been found on 29 farms in England; in the past few weeks they found it in sheep, but announced hey have identified it in cattle as well. In mainland Europe, it has been identified on several hundred farms in the Netherlands, Germany, Belgium, and France. The European Center for Disease Prevention and Control said the new virus’s closest relatives do not cause disease in humans — but that other more distantly related viruses do. The viral vector is believed to be midges and mosquitoes. The disease does not pass from adult animal to another animal, but apparently does from a mother animal to offspring in utero, and that is why it is showing up now: It is lambing season. With Europe enduring its coldest winter in decades, there are no virus-carrying insects flying around now. Instead, the animals giving birth to deformed and dead offspring were infected last summer and fall. No one has been able to say so far whether the organism can survive in insects over the winter. Agricultural media are starting to record the economic fallout, including a Russian ban on European livestock, and the possibility of a ban on shipping live animals and sales. Source: http://www.wired.com/wiredscience/2012/02/schmallenberg-virus/

Government Sector (including Schools and Universities)

Romanian man charged with hacking NASA computers. A Romanian man accused of hacking into NASA computers at the Jet Propulsion Laboratory (JPL) near Los Angeles under the online moniker "Iceman" was indicted on a federal charge, prosecutors said February 8. The man is charged with hacking into 25 NASA computers at JPL in December 2010, causing $500,000 in damage and leaving researchers unable to use them for 2 months, a U.S. attorney's spokesman said. The computers were part of the Atmospheric Infrared Sounder Program, which is used to support climate research and improve weather forecasting, he said. If convicted, the man faces a maximum sentence of 10 years in prison. Source: http://www.reuters.com/article/2012/02/09/us-nasa-hacking-idUSTRE81803S20120209

(New York) **Man shot, killed after opening fire at NY court.** A man killed in a gunfight with security officers at a courthouse in Middletown, New York, February 8 was convicted the week of January 30 for menacing the mayor's daughter and was angry at the mayor, according to authorities and court documents. The man opened fire with a 12-gauge shotgun in the lobby of his hometown courthouse at about 9 a.m. Officers returned fired as people in the building dove under desks and scrambled for the rear door, authorities said. The man died at a hospital. One of the officers suffered a graze wound to the arm, and two others were treated for shock. Source: http://online.wsj.com/article/APdfa2bd48894b4216b99ceff3dbb75b59.html

(California) **Anonymous targets Oakland officials over handling of Occupy.** The hacker group Anonymous released personal information of officials in Oakland, California, in a leak it said was in retaliation for the city's treatment of Occupy protesters, and officials February 7 decried the move as despicable. The hacker group released the home addresses, phone numbers, and names of relatives of Oakland's top elected officials the week of January 30, accompanied by a statement that they were "shocked and disgusted" by the treatment of protestors. In a press conference February 7, city officials pushed back against the leak. Oakland has been a flashpoint for the national "Occupy" protests against economic inequality that began in 2011 in New York's financial district and spread to dozens of cities. Source: http://www.chicagotribune.com/news/sns-rt-us-anonymous-oaklandtre8170b3-20120207,0,983012.story

(Alaska) **North Pole man threatens terrorism against Alaska in extortion attempt troopers say.** A North Pole man February 3 tried to extort $85,000 from the state of Alaska by threatening to carry out acts of terrorism against several companies and state institutions, according to Alaska State Troopers. The man was arrested, according to troopers, who February 5 posted a notice about the arrest on the agency's activity log. He was arraigned on a felony charge of extortion. He reportedly contacted troopers in Fairbanks and wanted to negotiate a deal. The trooper report said the suspect attempted to extort $85,000 from the state "in exchange for not committing several acts of terrorism which [he] believes would have affected oil companies, credit card companies, cell phone companies, the University of Alaska and the Alaska State Trooper's ability to conduct day to day operations." Source: http://newsminer.com/bookmark/17413416-North-Pole-man-threatens-terrorism-against-Alaska-in-extortion-attempt-troopers-say

The U.S. President imposes freeze on Iran property in U.S. The White House moved to enforce tightened sanctions against Iran February 6 because of the country's suspect nuclear program, freezing all property of the Central Bank of Iran, other Iranian financial institutions, and the Iranian government in the United States. The new restrictions also raised new warnings to financial institutions in other nations that they could face big penalties in the United States if they did business with Iran's central bank. The actions were announced in an executive order signed by the U.S. President that started the enforcement process for a tough measure he signed into law at the end of 2011. In a statement, the White House said the executive order "re-emphasizes this administration's message to the government of Iran — it will face ever-increasing economic and diplomatic pressure until it addresses the international community's...concerns regarding the nature of its nuclear program." Many countries buy oil from Iran through its central bank, and their financial institutions could be blocked from the American market if they continue to do so. Documents accompanying the executive order said foreign financial institutions risked American sanctions "if they engage in certain significant financial transactions" with Iran's central bank rather than "arms-length" transactions. In a statement, the Treasury Department said the executive order "blocks all property and interests in property of the government of Iran, the Central Bank of Iran and all Iranian financial institutions (regardless of whether the financial institution is part of the government of Iran) that are in the United States, that come within the United States or that come within the possession or control of U.S. persons." The statement did not further specify the exact properties that apply. Source: http://www.nytimes.com/2012/02/07/world/middleeast/white-house-moves-to-tighten-sanctions-on-iran.html?_r=1

Virus hits part of U.S. Commerce Dept. A virus caused the U.S. Department of Commerce's Economic Development Administration (EDA) to disable its e-mail and Internet access indefinitely while the nature and origin of the attack was investigated, InformationWeek reported February 3. Visitors to the EDA's Web site were greeted with a banner across the top with the message the agency's site and e-mail system is "experiencing a disruption in service." A Commerce spokeswoman confirmed the department isolated the network and systems by disconnecting them out of caution January 24, after a virus attack. The attack is still under investigation by the department's IT team, the United States Computer Emergency Readiness

Team, and an outside team of experts. Officials do not have details on the scope of the attack nor do they know when the systems will be back online, she said. The virus initially was discovered January 20, after which EDA IT staff issued McAfee system updates to all EDA staff computers over the next several days. However, the EDA discovered additional contamination, which led to disconnection of the systems. Source: http://www.informationweek.com/news/government/security/232600258

U.S. closes embassy in Syria. The U.S. State Department shuttered its embassy in Syria and pulled out its remaining staff February 6 after the government refused to address its security concerns, senior State Department officials told CNN. The officials said 17 employees, including the ambassador, left the country. Two employees flew out of the Syria the week of January 30, by commercial air, with the rest of them, including the ambassador, traveling by convoy February 6 to Jordan. Most of the staff were evacuated earlier in 2012, and the diplomatic team was further reduced in December 2011. The Syrians were notified about the decision to pull the staff and shutter the embassy after the employees were out of the country, the officials said. The officials said the deterioration of the situation in the country made it impossible for the embassy to continue operations and for staff members to remain. Source: http://security.blogs.cnn.com/2012/02/06/breaking-u-s-closes-embassy-in-syria/

Information Technology and Telecommunications

DDoS tools flourish, give attackers many options. According to a research analyst at Arbor Networks, there is now a thriving distributed denial of service (DDoS) tool and botnet ecosystem that includes single user flooding tools, small host booters, shell booters, remote access Trojans (RATs) with flooding capabilities, simple DDoS bots, complex DDoS bots, and some commercial DDoS services. Many types of threats can be blended into any given tool to make the tool more attractive and financially lucrative for whoever is renting out the DDoS capabilities. The researcher recently counted 55 different DDoS tools, which are just a fraction of what is publicly and commercially available. Some are more dangerous than others. For example, Fg Power DDOSER is designed to flood a gaming competitor with packets, slowing connection speed or knocking them offline, although the DDoS toolkit also includes a Firefox password stealer, he said. Another simple tool, Silent-DDoSer, can launch UDP, SYN, and HTTP attacks, and also offers “triple-DES and RC4 encryption, IPv6 capabilities, and password-stealing functions,” he said. At the other end of the spectrum, there are many complex DDoS toolkits and related bots, and typically also Web-based command-and-control interfaces. These toolkits sport names such as Darkness/Optima, DeDal, Dirt Jumper, G-Bot, and Russian Armageddon. Finally, services such as Death DDoS Service and Totoro offer commercial DDoS options, meaning that rather than running the tools themselves, attackers can outsource the job. Source: http://www.informationweek.com/news/security/attacks/232600497

‘Factory outlets’ selling stolen FebooTwitter credentials at discount rates. Stealing credentials via trojans has become so simple and prevalent that cybercriminals are finding themselves with a surplus: Two cybercrime gangs are now advertising bulk-rate Facebook, Twitter, and cPanel credentials in order to clean out their inventory. Researchers at Trusteer said these credential factory outlets are a way for the bad guys to cash in on other credentials thepilfered while stealing online banking credentials. It is like making money off the chafthat comes along with the valuable online banking credentials lifted by trojans and keyloggers: “They harvest a lot of things” unrelated to the stolen online banking credentials, said the vice president of marketing for Trusteer. “This is how they monetize the [leftover] assets they harvest.” The ads were running in underground forums infiltrated by the researchers from Trusteer. Trusteer believes attackers could lure users to those sites via phishing e-mails and social networking messages. Source: http://www.darkreading.com/advanced-threats/167901091/security/client-security/232600511/

New tool will automate password cracks on common SCADA product. Researchers are planning a February 14 release of tools that make it easy to test and exploit vulnerable programmable logic controllers (PLCs) and other industrial control systems. Among the releases will be a tool for cracking passwords on ECOM programmable logic controllers by Koyo Electronics, a Japanese firm, said a researcher at Digital Bond. Writing February 8, he said a February 14 release would include a “module to brute-force” passwords for ECOM and ECOM100 PLCs. Researchers revealed those devices have limited password space (forcing customers to implement short, weak passwords) and no lockout or timeout feature to prevent multiple log-in attempts used in brute force attacks. The Koyo ECOM models were among many popular PLC brands analyzed by top supervisory control and data acquisition security researchers as part of Project Basecamp. Their work revealed significant security issues with every system, with some PLCs too brittle and insecure to even tolerate security scans and probing. The Koyo ECOM100 modules were foundto come with a bundled Web server that contained denial of service and cross site scripting vulnerabilities, and an administrative panel that could be accessed without authentication. Organizers already released two modules for the Metasploit and Nessuvulnerability testing tools that can search for vulnerabilities discovered in D20 PLCs made by GE and promised more in February. Source: http://threatpost.com/en_us/blogs/new-tool-will-automate-password-cracks-common-scada-product-020812

iPhone bug enables FaceTime, shows names on locked phones. iPhones that have been password-protected and have voice dialing deactivated can still make FaceTime video calls, as well as disclose basic information about a person’s list of contacts. The security loophole, which is present in the latest version of Apple’s iOS 5.0.1 software, was discovered earlier the week of February 6 by a Canadian tech writer. CNET confirmed it working on three different iPhones, including the iPhone 4 and 4S. Source: http://news.cnet.com/8301-1009_3-57373491-83/iphone-bug-enables-facetime-shows-names-on-locked-phones/

Apple iWork passwords cracked. ElcomSoft can now recover passwords protecting Apple iWork documents. This makes Distributed Password Recovery the first tool to recover passwords for Numbers, Pages, and Keynote apps. “The recovery process is painfully slow,” comments ElcomSoft’s CTO. “Apple used strong AES encryption with 128-bit keys, which makes password attack the only feasible solution. We’re currently able to try several hundred password combinations per second on an average CPU. This is slow, and thus only distributed attacks can be used to achieve a reasonable recovery time. However, the human factor and our product's advanced dictionary attacks help recover a significant share of these passwords in a reasonable timeframe." Source: http://www.net-security.org/secworld.php?id=12376

Malware steals documents and uploads them to Sendspace. Security experts came across a piece of malware programmed to steal documents from the infected computer. The malicious element is designed to upload the obtained Microsoft Word and Excel files to the hosting site sendspace.com Trend Micro researchers said Sendspace was used previously to store stolen data because the service allowed crooks to "send, receive, track and share" big files, but the process was never done automatically by malware. The infection begins with an executable file called Fedex_Invoice(dot)exe, identified as TROJ_DOFOIL.GE, the file's name hinting it may be spread with the use of a fake "FedEx failed delivery" spam campaign. Once the file is executed, it downloads and executes TSPY_SPCESEND.A, a trojan that searches the local drive for Word and Excel documents, collecting them in a password-protected archive placed in the user's temporary folder. After the archive is created, it is uploaded to Sendspace, its download link transmitted to the malware's command and control (C&C) server. This way the crooks do not have to store all the files on the C&C, instead they access them from the file hosting service. This discovery means information theft and exfiltration are not specific only for targeted attacks, but they are present in mass campaigns as well. Source: http://news.softpedia.com/news/Malware-Steals-Documents-and-Uploads-Them-to-Sendspace-251430.shtml

FBI declares cloud vendors must meet CJIS security rules. The FBI February 7 reaffirmed its rule that all cloud products sold to to U.S. law enforcement agencies must comply with the FBI's Criminal Justice Information Systems (CJIS) security requirements. While the nation's top law enforcement agency conceded some vendors may have a tough time meeting those rules, it insisted there would be no compromising on security. The CJIS database, maintained by the FBI, is one of the world's largest repositories of criminal history records and fingerprints. The records are available to law enforcement agencies and contractors around the country that comply with the security rules, which include requirements that all data, both in transit and at rest, be encrypted and that anyone who accesses the database pass FBI background checks. A spokesman for the FBI's CJIS division February 7 maintained the CJIS security requirements are compatible with cloud computing. Source: http://www.computerworld.com/s/article/9224048/FBI_declares_cloud_vendors_must_meet_CJIS_security_rules?taxonomyId=17

Cisco recalls suicidal UCS blade servers. The week of January 30, Cisco Systems put out a field notice to customers using its Unified Computing System B440 server blades, stating the failure of a MOSFET power transistor on the blade can "cause the component to overheat and emit a short flash which could lead to complete board failure." The company said "in extreme circumstances it could affect the other blades in the chassis by disrupting power flow." Cisco warned customers something was wrong with the MOSFETs July 12, and said at that time there was "no indication of a systemic issue with the MOSFET components, and the observed failure in the field is considered to be a random component failure." To that end, Cisco's system engineers could issue a firmware fix for the blade to keep the MOSFET from overheating and flashing, causing the system board to fail. On January 26, Cisco notified customers using the B440 servers the firmware patch did detect MOSFET failures and prevent a "potential thermal event," but since the firmware was distributed, another B440 in the field failed. As a result, Cisco made hardware modifications to the B440 system board and is now replacing all machines currently used by customers. Cisco said in the field notice no other UCS B Series blade servers or C Series rack servers are affected by this MOSFET failure issue. For users with these B440s in production, Cisco recommends upgrading to the most recent UCS blade management controller software, which has the patch for monitoring the B440 MOSFETs, and arranging to get replacement blades as soon as possible. Source: http://www.theregister.co.uk/2012/02/06/cisco_b440_server_recall/

Anonymous claims to have released source code of Symantec's pcAnywhere. Hacker group Anonymous claimed February 6 the source code of Symantec's pcAnywhere was uploaded on The Pirate Bay site. Symantec could not immediately comment on whether the hackers indeed released the source code of its product. Earlier February 6, an e-mail string posted on Pastebin referred to negotiations over payment for the source code between a purported Symantec employee and a person named Yamatough. The name of the hacker is similar to the Twitter handle of YamaTough in Mumbai who is associated with the hacker group, Lords of Dharmaraja, that earlier claimed it had access to the source code of some Symantec products. Source: http://www.computerworld.com/s/article/9224016/Anonymous_claims_to_have_released_source_code_of_Symantec_s_pcAnywhere?taxonomyId=17

Facebook malware scam takes hold. A large number of Facebook users were sharing a link to a malware-laden fake CNN news page reporting the United States attacked Iran and Saudi Arabia, security firm Sophos said February 3. If users who follow the link click to play what purports to be video coverage of the attack, they are prompted to update their Adobe Flash player with a pop-up window that looks like the real thing. Those who accept the prompt unwittingly install malware. Within 3 hours of the scam's appearance, more than 60,000 users followed a link to the spoofed CNN page, according to a Sophos senior security adviser. Facebook removed that link, but others were still being shared. In a statement, Facebook said it was "in the process of cleaning up this spam now, and remediating any affected users." Source: http://www.computerworld.com/s/article/9223976/Facebook_malware_scam_takes_hold?taxonomyId=17

State of SCADA security worries researchers. Recent reports painted a bleak picture of the security issues plaguing industrial control systems, but the situation is exacerbated by the fact administrators are naive about the dangers, researchers said. Researchers presented some alarming findings about the state of security for supervisory control and data acquisition (SCADA) systems at the Kaspersky Security Analyst Summit February 3. SCADA systems are used across varied industries such as oil, water systems, electric grids, controlling building systems, and the basic security model underlying these systems is completely inadequate, they said.

Source: http://www.eweek.com/c/a/Security/State-of-SCADA-Security-Worry-Researchers-234517/

PHP 5.3.9 regression allows HTTP header attacks and 32/64-bit OS detection. After the PHP Group fixed the hash collision issue by releasing a patch to mitigate attacks, the fix turned out to be problematic, with xperts identifying a remote code execution vulnerability. Now, it turns out the same variant opened up the possibility of a new class of HTTP header attacks. The security expert who found the remote code execution flaw also uncovered this second issue. He believes the max_input_vars variable initially limited to a maximum number of 1,000 to mitigate hash collision attacks allows the identification of 32-bit and 64-bit operating systems introducing the possibility of this header attack that eventually leads to remote code execution. Knowing this information, allows attackers of remote memory corruption vulnerabilities to better prepare for the target he said. While the issue affects nearly all PHP applications, he claims Suhosin Extension users are safe from this issue, and a new feature will be added to protect against HTTP header attacks. Source: http://news.softpedia.com/news/PHP-5-3-9-Regression-Allows-HTTP-Header-Attacks-and-32-64-Bit-OS-Detection-250872.shtml

National Monuments and Icons

(California) **Copper wire thieves target state parks.** Copper wire thieves are narrowing in on state parks, KTVU 2 Oakland reported February 4. A California state park ranger said thieves damaged one area of a state park in Benicia by digging a hole to rip out buried copper wires. A bathroom at Dillon’s Point was left with no electricity because of the vandals. A ranger who patrols the grounds said that in less than a year, thieves have caused $30,000 worth of damage. State park officials have contacted recycling centers and asked them to keep an eye out for the stolen copper. Source: http://www.ktvu.com/news/news/copper-wire-thieves-target-state-parks/nHTjx/

(District of Columbia) **Park police sweep occupy sites.** U.S. Park Police inspected and removed tents from Freedom Plaza in Washington D.C. February 5, one day after sweeping through Occupy D.C.’s McPherson Square protest site. Park police stressed that they were not evicting protesters, and wanted to respect their First Amendment rights. The National Park Service, which oversees McPherson Square and Freedom Plaza, has maintained that protesters are allowed to hold 24-hour vigils on its grounds, but are not allowed to camp out. At least one officer was injured after a protester threw a brick at his face as authorities removed tents from the Occupy D.C. protest site February 4. The officer was treated for facial injuries and released from an area hospital. The protester who threw the brick was arrested and charged with felony assault on a police officer and assault with a deadly weapon. In all, 12 people were arrested in the park the weekend of February 4. The McPherson Square removal operation, which lasted through the day and into the night, began after protesters agreed to a request from U.S. Park Police to remove a giant tarp called the “Tent of Dreams”. Later, police in biohazard suits began to break down tents around the campsite, encountering little resistance. A federal judge ruled earlier in the week of January 30 that Occupy D.C. would need to be notified if the government intended to evict them and could challenge any planned eviction. Source: http://www.msnbc.msn.com/id/46262652/ns/local_news-washington_dc/#.Ty_xIMj4XTo

Postal and Shipping

Anthrax mailings recovery required $320M, analysis finds. The 2001 anthrax mailings resulted in $320 million in expenditures aimed at ensuring government and private facilities were free of the deadly bacteria, according to an analysis published February 7. The anthrax-tainted letters addressed to Congressional offices and media organizations killed five people and sickened 17, according to a previous report. After reviewing U.S. Government Accountability Office information and other material, experts at Concordia University in Montreal determined the mailings resulted in follow-up detection efforts in 26 structures and cleansing operations in seven, including two mail service centers that required an expensive decontamination treatment, the Center for Infectious Disease Research and Policy reported. In addition, six business facilities required cleaning. Source: http://www.nti.org/gsn/article/anthrax-mailings-recovery-required-320m-analysis/

Public Health

Lyme disease high-risk areas revealed in new map. An extensive field study has identified areas of the United States where people have the highest risk of contracting Lyme disease, according to the Centers for Disease Control and Prevention. The study found that high infection risk is mainly confined to the Northeast, Mid-Atlantic and Upper Midwest regions. To collect data for the study, scientists studied 304 sites from Maine to Florida, and across the Midwest, between 2004 and 2007. At each location, “tick hunters” combed for Lyme disease-carrying ticks called black-legged ticks. The findings showed a heightened risk of Lyme disease in large parts of the Northeast, from Maine going as far south as Maryland and northern Virginia. The researchers also identified a separate and distinct Lyme disease risk region in the upper Midwest that includes most of Wisconsin, a large area in northern Minnesota, and a sliver of northern Illinois. The researchers noted the study did not examine risk in the West, where Lyme disease is believed to be confined to areas along the Pacific Coast, and where a different tick species, known as the western black-legged tick, carries the bacteria. The South was rated as having a low infection risk, according to the survey findings. The study is published in the February issue of the American Journal of Tropical Medicine and Hygiene. Source: http://www.foxnews.com/health/2012/02/07/lyme-disease-high-risk-areas-revealed-in-new-map/

Noroviruses leading cause of hospital infections. Norovirus outbreaks are the leading cause of infection outbreaks in hospitals, particularly in the non-acute care setting, and often lead to unit closure, data published in the American Journal of Infection Control February 6 indicate. Researchers conducted a two-part electronic survey of infection preventionists to determine the frequency of outbreak investigations in U.S. hospitals over a 24-month period, as well as to collect data on specific investigations, including control measures. A total of 882 responses were received, which provided data on 386 outbreaks in 289 hospitals. Researchers found four organisms were responsible for nearly 60 percent of infectious disease outbreaks: noroviruses accounted for 18 percent, Staphylococcus aureus for 17 percent, Acinetobacter spp for 14 percent and Clostridium difficile for 10 percent. Norovirus outbreaks predominated in behavioral health and rehabilitation/long-term care facilities, whereas bacterial infections caused by the other three organisms were more likely to occur in medical and surgical units. Units in which outbreaks occurred were closed in 22.6 percent of cases, with norovirus pathogens most often associated with closure. Source: http://www.clinicaladvisor.com/noroviruses-leading-cause-of-hospital-infections/article/226492/

Transportation

Congress passes bill to speed air traffic control switch to GPS, open skies to drone aircraft. A bill to speed the nation's switch from radar to an air traffic control system based on GPS technology, and to open U.S. skies to unmanned drone flights within 4 years, received final Congressional approval February 6. The bill, which has been sent to the U.S. President for his signature, authorizes $63.4 billion for the Federal Aviation Administration (FAA) over 4 years, including about $11 billion toward the air traffic system and its modernization. It accelerates the modernization program by setting a deadline of June 2015 for the FAA to develop new arrival procedures at the nation's 35 busiest airports so planes can land using the more-precise GPS navigation. Source: http://www.washingtonpost.com/business/technology/senate-passes-faa-bill-that-speeds-switch-to-gps-opens-us-skies-to-unmanned-aircraft/2012/02/06/gIQAvU7vuQ_story.html

(California) **Plane stolen from Concord airport crashes, 1 dead.** A single-engine airplane stolen from Buchanan Field crashed February 5 in Fresno County, California, killing the pilot. The owner of the Cessna 172 called the Contra Costa Sheriff's Office February 5 after hearing from Fresno investigators. He noticed it missing February 4, a Contra Costa sheriff's spokesman said, but figured it was being serviced. The owner of the plane last saw it February 3 at the Concord airport. It crashed into the bank of a canal west of Fresno about 4 p.m. February 5. Source: http://www.mercurynews.com/news/ci_19906486

(Ohio; West Virginia) **Corrosion threat on Skyway bridge deck discovered.** Grout packed into bundles of steel cables that compress together the concrete deck sections of the Veterans' Glass City Skyway in Toledo, Ohio, may contain elevated levels of salts that would cause those cables to corrode prematurely, the grout's manufacturer warned the Ohio Department of Transportation. The I-280 bridge over the Maumee River, which opened 5 years ago, is one of several dozen projects across the United States that used grout made at a Marion, Ohio, plant owned by Sika Corp. U.S. in which excessive chloride compounds, traced to cement the plant bought from an unnamed supplier, have been discovered. Also potentially affected is the Perry Street bridge in Napoleon, which carries State Rt. 108 over the Maumee and was replaced in 2005, the U.S. 33 bridge over the Ohio River between Pomeroy, Ohio, and Mason, West Virgina, and as many as eight other smaller bridges in Ohio. The planning and engineering administrator at the transportation department's district office in Bowling Green, said about 30 projects were affected overall. In the worst case, transportation and company officials said, chloride presence would not create an imminent — or even short-term — safety hazard on the $273 million bridge built between 2002 and 2007. But there is the possibility, they said, that as the bridge ages, chloride in the grout could cause the cables — known formally as “post-tensioning tendons” — to corrode and fail sooner than they otherwise would. Source: http://www.toledoblade.com/local/2012/02/06/Corrosion-threat-on-Skyway-bridge-deck-discovered.html

Water and Dams

(California) **Water-quality plan for L.A., Long Beach ports approved.** State water regulators approved a plan to restore water quality at the ports of Los Angeles and Long Beach, California by putting limits on 70 pollutants that contaminate water and sediment and make fish toxic to eat. The plan passed February 7 by the state water board will cap the amount of toxic metals and chemicals such as DDT and PCBs allowed in the sediment, water, and fish in the nation’s largest shipping complex. The plan aims to reduce pollution in the ports and the Dominguez Channel over the next 20 years by cleaning up toxic “hot spots” where pollutants have accumulated in the harbor bottom. It will also require that neighboring cities ensure they are not adding to the contamination by discharging dirty stormwater into the port complex. The buildup of metals, pesticides, and other toxic chemicals in fish is such a problem in Southern California waters that health officials in 2009 expanded the number of fish on the “do not eat” list from one to five species. From Santa Monica to Seal Beach, white croaker, barracuda, topsmelt, black croaker, and barred sand bass are considered so contaminated with the banned pesticide DDT, toxic chemicals known as PCBs, and poisonous mercury they are unsafe for human consumption. The state’s water quality plan will require regular monitoring and testing for pollutants in the harbor complex and in the tissue of sport fish. To take effect, the plan must be given final approval by the U.S. Environmental Protection Agency. Source: http://latimesblogs.latimes.com/lanow/2012/02/toxic-water-and-fish-restoration-plan-approved-for-la-long-beach-ports.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+lanowblog+(L.A.+Now)&utm_content=Google+Feedfetcher

(California) **Report backs $1 billion plan to raise dam; Some relocation is necessary, but agriculture, wildlife benefit.** A draft report released February 6 by federal officials said a $1.07 billion plan to raise Shasta Dam in Shasta County, California, by 18.5 feet is feasible and justifiable. Raising the dam would increase the lake’s storage about 14 percent, benefiting agricultural and municipal water users in the state, according to the Shasta Lake Water Resources Investigation draft feasibility report. It would also benefit fish that migrate up the Sacramento River, the feasibility report said. However, some roads, buildings, and businesses around the lake would be inundated by the higher lake level, said a spokesman for the U.S. Bureau of Reclamation, the agency that prepared the report. Raising the dam height 18.5 feet would actually increase the depth of the lake 20 feet, the report said. “Although higher dam raises are technically feasible, 18.5 feet is the largest dam raise that would avoid extensive and costly relocations, including moving the Pit River Bridge and Interstate 5,” the report said. With a higher dam and the lake full, water levels would be just 4 feet from the bottom of the Pit River Bridge, the report said. Source: http://www.redding.com/news/2012/feb/06/report-backs-1-billion-plan-to-raise-dam-raising/

(Tennessee) **Prosecutors said waste water potentially put public at risk.** The operator of a Niota, Tennessee water treatment plant must serve 6 months in a federal prison for falsifying documents that covered up his failure to properly operate a sewage treatment system. Before the sentencing February 6, federal prosecutors asked the court to make an example out of the operator, arguing he potentially put the public at risk of contracting serious illnesses. They said the man failed to properly disinfect wastewater before it was discharged into Little North Mouse Creek, a tributary of the Hiwassee River. A federal judge also ordered the man to serve 6 months on home detention following his release from prison and to perform 150 hours of community service. He pleaded guilty in September 2011 to 12 counts of falsifying documents required by the Federal Clean Water Act. Source: http://www.therepublic.com/view/story/841c90e1c9b54380a31c5dd8d88e288e/TN--Sewage-Operator-Sentenced/

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168